

CLAIMS:

- 5 *Sub*
1. A method for identifying a device acting as a server on a network, the method comprising:
- receiving data representing communications on the network, the data containing source device, destination device, data transfer protocol and data volume information for communications represented therein;
- identifying data relating to one or more relevant server protocols, and
- using the identified data, determining as a server device, the device which has
- 10 the highest data volume for communications in which it is the source or destination device and which communications involve at least a threshold number of other devices.
2. A method as claimed in claim 1, wherein the step of identifying data relating
- 15 to relevant server protocols comprises:
- for each communication included in the management data, comparing the data transfer protocol with at least one predefined server protocol, and
- when the comparison results in a match, identifying the corresponding management data as relating to a relevant server protocol.
- 20 3. A method as claimed in claim 2, wherein the step of identifying further includes marking the identified data.
4. A method as claimed in claim 1, further comprising:
- 25 after the step of identifying data relating to relevant server protocols, identifying the devices involved in the communications represented in the identified data using the source device and destination device information, and
- for each identified device, determining the total volume of data transferred during communications represented in the identified data involving the device using
- 30 the volume information.

0541407 081700

5. A method as claimed in claim 4, further comprising:
after the step of determining the total volume of data transferred for each device, identifying the device with the highest total volume.

5 6. A method as claimed in claim 5, further comprising:
after the step of identifying the device with the highest total volume, determining the number of other devices involved in communications, represented in the identified data, with the identified device.

10 7. A method as claimed in claim 6, further comprising:
after the step of determining the number of other devices, comparing the determined number against a predetermined threshold number, and
if the determined number exceeds the predetermined threshold number, determining that the identified device with the highest total volume is a server device.

15 8. A method as claimed in claim 7, further comprising:
removing data representing communications involving the determined server device from the identified data.

20 9. A method as claimed in claim 8, wherein the step of removing comprises unmarking the data.

10. A method as claimed in claim 1, wherein the received data comprises network traffic data.

25 11. A method as claimed in claim 10, further comprising, prior to the step of receiving, collecting said network traffic data at a location on the network using a network device selected from the group consisting of: managed network devices; traffic monitors; firewalls and packet capture devices.

30

09644407 "081700

12. A method as claimed in claim 11, wherein the data is collected over a predetermined time period.

13. A method as claimed in claim 11, wherein the network traffic data is RMON2 data.

14. A method as claimed in claim 1, wherein the threshold number is an integer greater than one.

15. A method as claimed in claim 1, wherein the relevant server protocols are selected from the group consisting of: HTTP; FTP; SMTP; Notes; DNS; IPX; SAP; Oracle; SIP; HTTPS; NetBeui; NFS; NetBios; NCP; SMB and H323.

16. On a computer readable medium, a computer program comprising:

program means for receiving data representing communications on the network, the data containing source device, destination device, data transfer protocol and data volume information for communications represented therein;

program means for identifying data relating to one or more relevant server protocols, and

program means, using the identified data, for determining as a server device, the device which has the highest data volume for communications in which it is the source or destination device and which communications involve at least a threshold number of other devices.

17. A computer program as claimed in claim 16, wherein the program means for identifying data relating to relevant server protocols comprises:

program means for comparing, for each communication included in the management data, the data transfer protocol with at least one predefined server protocol, and

program means for identifying the corresponding management data as relating to a relevant server protocol, when the program means for comparing determines a match.

5 18. A computer program as claimed in claim 17, further comprising program means for marking the identified data.

19. A computer program as claimed in claim 16, wherein the program means for determining as a server device further comprises:

10 program means for identifying, after identifying data relating to relevant server protocols, the devices involved in the communications represented in the identified data using the source device and destination device information, and

15 program means for determining, for each identified device, the total volume of data transferred during communications represented in the identified data involving the device using the volume information.

20. A computer program as claimed in claim 19, wherein the program means for determining as a server device further comprises:

20 program means for identifying, after said determining, the total volume of data transferred for each device, the device with the highest total volume.

21. A computer program as claimed in claim 20, wherein the program means for determining as a server device further comprises:

25 program means for determining, after said identifying, the device with the highest total volume the number of other devices involved in communications, represented in the identified data, with the identified device.

22. A computer program as claimed in claim 21, further comprising:

30 program means for comparing, after said determining the number of other devices, the determined number against a predetermined threshold number, and

002780" 20474960

program means for determining, if the determined number exceeds the predetermined threshold number, that the identified device with the highest total volume is a server device.

- 5 23. A computer program as claimed in claim 22, further comprising:
 program means for removing data representing communications involving the determined server device from the identified data.

- 10 24. A computer program as claimed in claim 16, wherein the received data comprises network traffic data, the program further comprising:
 program means for retrieving said network traffic data from a network device at a location on the network, and
 program means for storing the data in a data table in the form:
 [source], [destination], [application], [volume].

- 15 25. A computer program as claimed in claim 24, the network traffic data is RMON2 data.

- 20 26. Apparatus for identifying a device acting as a server on a network, the apparatus comprising:
 a network device for collecting data representing communications on the network, the data containing source device, destination device, data transfer protocol and data volume information for communications represented therein; and
 a processor for receiving the data and for identifying data relating to one or
 more relevant server protocols, said processor using the identified data to determine
 as a server device, the device which has the highest data volume for communications
 in which it is the source or destination device and which communications involve at
 least a threshold number of other devices.

- 30 27. Apparatus as claimed in claim 26, further comprising:
 a data storage for storing the data in a data table having the fields:

002780" 20474950

15

[source], [destination], [application], [volume].

28. Apparatus as claimed in claim 27, wherein the data storage comprises a database.

5

09541407.081700